LIST OF REFERENCES

1... transaction authentication system

11... orderer terminal

11a... authentication request input unit

11b... authentication request transmission unit

11c... authentication reply reception unit

11d... authentication request encryption unit

11e... authentication reply decryption unit

12... bio-authentication apparatus

13... authentication apparatus

13a... authentication request reception unit

13b... orderer authentication unit

13c... request generation unit

13d... reply transmission unit

13e... reply reception unit

13f... vendor authentication unit

13g... authentication reply generation unit

13h... authentication reply encryption unit

13i... authentication reply transmission unit

13j... request encryption unit

13k... reply decryption unit

13l... authentication request decryption unit

14... authentication log storage unit

15... vendor terminal

15a... authentication reply reception unit

15b... request decryption unit

15c... reply input unit

15d... reply generation unit

15e... reply encryption unit

15f... reply transmission unit

101... transaction authentication system

1011... orderer terminal

1011a... authentication request input unit

1011b... authentication request transmission unit

1011c... authentication reply reception unit

101d... authentication request encryption unit

101e... authentication reply decryption unit

12... bio-authentication apparatus

113... authentication apparatus

113a... authentication request reception unit

113b... orderer authentication unit

113c... request generation unit

113d... reply transmission unit

113e... reply reception unit

113f... vendor authentication unit

113g... authentication reply generation unit

113h... authentication reply encryption unit

113i... authentication reply transmission unit

113j... request encryption unit

113k... reply decryption unit

1131... authentication request decryption unit

14... authentication log storage unit

15... vendor terminal

115a... authentication reply reception unit

115b... request decryption unit

115c... reply input unit

115d... reply generation unit

115e... reply encryption unit

115f... reply transmission unit

201... transaction authentication system

211... orderer terminal

215... vendor terminal

31... orderer

33... vendor

240... network bank

250... authentication apparatus

261, 271, 281... reception unit

262, 272, 282... transmission unit

263, 273, 283... encryption unit

264, 274, 284... decryption unit

265, 275, 285... storage unit

266, 276, 286... control unit

267, 277... signature verification unit

287... signature preparation unit

288... charge processing unit

a1... order information

k1... personal key information k1 of orderer 31

ID1... personal ID information of orderer 31

ID_M... apparatus ID information

Au1, Au2... signature information of authentication apparatus

Z... information specifying vendor

Inf1... authentication request

Inf4... authentication reply

301... transaction authentication system

311... orderer terminal

315... vendor terminal

340, 341... network bank

350, 351... authentication apparatus

361, 371, 381, 391... reception unit

362, 372, 382, 392... transmission unit

363, 373, 383, 393... encryption unit

364, 374, 384, 394... decryption unit

365, 375, 385, 395... storage unit

366, 376, 386, 396... control unit

367, 377... signature verification unit

387, 397... signature preparation unit

388, 398... charge processing unit

a1... order information

k1... personal key information k1 of orderer 31

ID1... personal ID information of orderer 31

b1... information specifying vendor

Au-B... signature information of authentication apparatus 351

Au-A1, Au-A2... signature information of authentication apparatus 350

Z... information specifying vendor

1301... transaction authentication system

1311... orderer terminal

1315... vendor terminal

1340, 1341... network bank

1350, 1351... authentication apparatus

1361, 1371, 1381, 1391... reception unit

1362, 1372, 1382, 1392... transmission unit

1363, 1373, 1383, 1393... encryption unit

1364, 1374, 1384, 1394... decryption unit

1365, 1375, 1385, 1395... storage unit

1366, 1376, 1386, 1396... control unit

1367, 1377... signature verification unit

1387, 1397... signature preparation unit

1388, 1398... charge processing unit

a1... order information

k1... personal key information k1 of orderer 31

ID1... personal ID information of orderer 31

b1... information specifying vendor

Au-B1, Au-B2... signature information of authentication apparatus 1351

Au-A1, Au-A2... signature information of authentication apparatus 1350

Z... personal key information of information specifying vendor

401... transaction authentication system

411... orderer terminal

415... vendor terminal

440... network bank

450... authentication apparatus

461, 471, 481... reception unit

462, 472, 482... transmission unit

463, 473, 483... encryption unit

464, 474, 484... decryption unit

465, 475, 485... storage unit

466, 476, 486... control unit

467, 477... signature verification unit

487... signature preparation unit

488... charge processing unit

a1... order information

k1... personal key information k1 of orderer 31

ID1... personal ID information of orderer 31

ID_N... network ID

Au1, Au2... signature information of authentication apparatus

Z... information specifying vendor

Inf1... authentication request

1nf4... authentication reply

501... transaction authentication system

511... orderer terminal

515... vendor terminal

540... network bank

550... authentication apparatus

561... external network I/F

562... internal network I/F

571, 581... reception unit

572, 582... transmission unit

563, 573, 583... encryption unit

564, 574, 584... decryption unit

565, 575, 585... storage unit

566, 576, 586... control unit

567, 577... signature verification unit

587... signature preparation unit

588... charge processing unit

a1... order information

k1... personal key information k1 of orderer 31

ID1... personal ID information of orderer 31

ID_{M1}, ID_{M2}, ID_{M3}, ID_{M4}, ID_{M56}... apparatus ID information

Au1, Au2... signature information of authentication apparatus

Z... information specifying vendor

Inf1... authentication request

1nf4... authentication reply

601... information storage apparatus

610... read circuit

611... encryption circuit

612... information division circuit

613, 614... write circuit

65, 616, 617... storage medium

620, 621... read circuit

622... information composition circuit

623... decryption circuit

624... write circuit

631... information decryption apparatus

641... information storage apparatus

650... read circuit

651... information division circuit

652, 653... decryption circuit

654, 655... write circuit

661... information decryption apparatus

670, 671... read circuit

672, 673... decryption circuit

674... information composition circuit

675... write circuit

801... authentication system

811... terminal

813... authentication apparatus

821... network bank

831... user

861, 881... reception unit

862, 882... transmission unit

863, 883... encryption unit

864, 884... decryption unit

865, 885... storage unit

866, 886... storage unit

867, 887... display unit

868, 888... control unit

869, 889... smart card access unit

901... transaction authentication system

911... orderer terminal

911a... authentication request input unit

911b... authentication request transmission unit

911c... authentication reply reception unit

911d... authentication request encryption unit

911e... authentication reply decryption unit

12... bio-authentication apparatus

913... authentication apparatus

913a... authentication request reception unit

913b... orderer authentication unit

913c... request generation unit

913d... reply transmission unit

913e... reply reception unit

913f... vendor authentication unit

913g... authentication reply generation unit

913h... authentication reply encryption unit

913i... authentication reply transmission unit

913j... request encryption unit

913k... reply decryption unit

913l... authentication request decryption unit

913m... settlement processing unit

914... authentication log storage unit

915... vendor terminal

115a... authentication reply reception unit

115b... request decryption unit

115c... reply input unit

1915d... reply generation unit

915e... reply encryption unit

915f... reply transmission unit